Section V:	**Physical Security**
Title:	**Asset and Inventory Control Standard**
Current Effective Date:	**June 30, 2008**
Revision History:	**May 13, 2008**
Original Effective Date:	**June 30, 2008**

Purpose: To define a strategy for Divisions and Offices of the North Carolina (NC) Department of Health and Human Services (DHHS) for developing an asset control system to ensure end-to-end accountability and security of property, equipment, media, and data.

STANDARD

1.0 Background

Asset control systems allow for day-to-day protection of assets as well as providing the means to readily identify issues of lost, stolen, or compromised assets. The assets of an organization need to be controlled and can be defined as all physical property, electronic equipment, and hard or softcopy data that is part of the system(s) used for protecting and securing confidential data created, used, received, disclosed, and/or maintained by that organization.

2.0 Asset Control Systems

Some safeguards and procedures that should be implemented as part of an asset control system are listed below but are not limited to:

- Develop a paper or electronic database system to inventory current assets and a method for adding new assets
- Inventory and document the disposition of current assets
- Identify and inventory any new assets or changes to the disposition of current assets as they occur
- Identify and verify current assets and the validity of the inventory annually

3.0 Disposition of Assets

The disposition of an asset is the specific use, physical location of, or the owner/user of an asset. Changes in the functional use, reuse, alternate use, or destruction of an asset shall be documented to identify, authorize, and control the use of property, equipment, media, and the production dissemination or storage of confidential data. Documentation of the disposition of assets shall be applied appropriately to physical equipment, electronic systems, and media or intangible data assets.

4.0 Physical Property and Equipment Control

4.1 Initial Property Accountability

Establishing control of existing equipment is the first important step in identifying and eliminating unauthorized equipment that may lead to a breach in the security posture of an organization. A comprehensive inventory of all information technology (IT), data processing/storage, duplication, transmission, audio/video and telecommunications equipment should be logged. In addition, a register of the location of the equipment, any identifying serial numbers, user name, and approving authority should be maintained. Once existing equipment is cataloged, unauthorized items can be identified and either removed from the facility or appropriately approved and added to the inventory.

4.2 Acquiring New Equipment

When acquiring new equipment for your organization it must first be approved for a specific use and meet minimum requirements for safety, if applicable. Once an item has been ordered, purchased, and received, it must be added to the existing inventory control system. The same process for identifying and logging existing property will be followed when new equipment is added (i.e. documenting the serial or other identifying number, description, location, approval authority, etc.) .

4.3 Property Identification

Asset tags are a critical part of maintaining control of equipment. Asset tags indicate that a specific piece of equipment is authorized to be in a particular area. An asset tag should indicate ownership and have a unique, sequential tracking number that can be used to maintain an inventory list and assure that there are no unaccounted-for or duplicate items.

5.0 Asset Lifecycle Control

5.1 Asset Reuse and Destruction

In order to appropriately control reuse or destruction of assets within an organization, an effective asset reuse process must be implemented. Proper documentation simplifies the process of determining when equipment is no longer adequate for the assigned use. Documentation shall include the current disposition of the equipment as well as any exchange requirements necessary to put the equipment into service with another user or group.

When equipment is identified as inadequate for its current assigned use it may be documented as a “turn-in” in the inventory control documentation. The equipment may be put back into service in another capacity with another user or group; however, if the equipment is deemed unusable it may be identified for “destruction”. When identifying equipment for either reuse or destruction, it shall be inspected for any residual data or documents and be sanitized in accordance with Section 6.5.

6.0 Electronic Media and Data Control

6.1 Data Protection

Information collected, stored, used, modified, or maintained by the Divisions or Offices shall be handled in accordance with the NC DHHS Security Standards, Administrative Security Standard -Data Stewardship.

6.2 Hard Data Control

The location of hard copy data shall be identified and documented to ensure comprehensive physical control of all data assets within a Division or Office. Storage and working areas for documents containing confidential data shall be appropriate to the sensitivity of the information. Filing cabinets equipped with locking devices shall be used and confidential data shall not be left unattended while not in use. When sensitive information is mailed, shipped, faxed, or otherwise transmitted, the correct recipient and delivery confirmation shall be verified.

6.3 Soft Data Control

When introduction of external data to an IT system is necessary, origin and authenticity of the information shall be verified through media inspection to ensure that:

- Requested data or files come from a known, trusted source
- No malicious or unauthorized software is downloaded
- Electronic media entering or leaving offices, processing areas, or storage facilities shall be appropriately controlled
- Delivery is verified when sensitive information is transferred to off-site storage
- Physical data protections required by the owning organization must be ensured at an off-site storage facility

6.4 Media and Data Destruction

If possible and appropriate, all soft or hard data that are marked for destruction shall be reviewed by management for authorization to destroy. Hard data no longer needed shall be destroyed via on-site shredding. Data destruction standards and accountability should be based on the sensitivity level of the information being destroyed and appropriate workforce members, such as records management staff who are familiar with records retention schedules, should be included in this process.

6.5 Soft Data Destruction

Soft data on media identified for reuse shall be purged by an appropriate method to completely delete all data including any residual metadata. All sanitized media should be reviewed and approved for reuse by the Division or Office ISO. Media formats commonly identified for reuse may include but are not limited to:

- USB Jump drive storage devices (aka thumb drives)
- CD-RW
- DVD-RW
- Magnetic tape
- Floppy disks

- Zip disks

Media meant for destruction shall be destroyed in accordance with accepted Department of Defense (DoD) standards. Below are some approved methods:

- Degaussing of hard drives
- Sanding or surface etching of hard drive platters
- Shredding, cutting, or chipping of CDs, DVDs, magnetic tape, floppy media, and zip disks

6.6 Emergency Safeguarding

Divisions or Offices shall develop procedures for safeguarding protected information in emergency situations. The procedures shall be as simple and practical as possible and should be adaptable to any type of emergency that may arise. Divisions or Offices shall incorporate these safeguards into their Business Continuity Plan (BCP). Divisions or Offices shall promptly report any emergency situation that renders the facility incapable of physically safeguarding protected information to the Division Information Security Official (ISO).

References:

- DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM): Chapter 8 - Information System Security

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 01 - Classifying Information and Data, Section 01: Setting Classification Standards,
    - Standard 010103 - Storing and Handling Classified Information
  - Chapter 03 - Processing Information and Documents, Section 02: System Operation and Administration
    - Standard 030203 - Controlling Data Distribution
  - Chapter 03 - Processing Information and Documents, Section 03: Email and the World Wide Web
    - Standard 030318, Certainty of File Origin
  - Chapter 03 - Processing Information and Documents, Section 05: Data Management, 030501 - Transferring and Exchanging Data
    - Standard 030505 - Receiving Information on Disks
  - Chapter 05 - Securing Software, Peripherals and Other Equipment, Section 01- Purchasing and Installing Hardware
    - Standard 050101 - Specifying Information Security Requirements for New Hardware
  - Chapter 05 - Securing Software, Peripherals and Other Equipment, Section 03: Consumables
    - Standard 050302 - Using Removable Storage Media, Including Diskettes and CDs
  - Chapter 05 - Securing Software, Peripherals and Other Equipment, Section 07: Other Hardware Issues
    - Standard 050701 - Disposing of Obsolete Equipment
    - Standard 050707 - Taking Equipment off the Premises

- NC DHHS Security Standards
  - Administrative Security Standards
    - Data Stewardship

- NC DHHS Policy and Procedures Manual, Section VIII - Security and Privacy, Security Manual
  - IT Inventory Management and Control Policy
  - Physical and Environmental Security Policy